CLAIMS

What is claimed is:

1. A system for generating an asymmetric crypto-key usable to transform messages to encrypt and decrypt or sign the messages for a user, comprising:

a first processor configured to (i) generate a private crypto-key and a corresponding public crypto-key associated with the user, (ii) divide the private crypto-key into a first private key portion, based on a password of the user, and a second private key portion, (iii) destroy the private crypto-key and the first private key portion without distribution thereof and without storage thereof in a persistent state, and (iv) store only the second private key portion and the public crypto-key in a persistent state; and

a second processor representing a user and configured to (i) generate, responsive to receipt of an inputting of and based on the user password, only the first private key portion, and (ii) destroy, without storing in a persistent state, the generated first private key portion.

2. A system according to claim 1, wherein the user password has a bit length of between 56 and 72 bits and the generated first private key portion has a bit length of at least 257 bits.

3. A system according to claim 1, wherein the first private key portion is generated in accordance with a one way function.

4. A system according to claim 3, wherein:

the first processor and the second processor are further configured to selectively operate in a first mode and a second mode;

in the first mode the first processor and the second processor apply the one way function a first number of times to generate the first private key portion; and

in the second mode the first processor and the second processor apply the one way function a second number of times, different than the first number of times, to generate the first private key portion.

5. A system according to claim 4, wherein:

the first processor and the second processor are further configured to select one of the first and second mode for operation based on at least one of an identity of the user and a strength of the user password.

6. A system according to claim 3, wherein:

the first processor and the second processor are further configured to select the one way function from a group of one way functions.

7. A system according to claim 6, wherein:

the first processor and the second processor are further configured to select the one way function based upon at least one of an identity of the user and a strength of the user password.

8. A system according to claim 1, wherein:

the second processor is further configured to encrypt or sign a message with the first private key portion prior to destroying the generated first private key portion; and the first processor is further configured to recover or verify the encrypted message by applying the stored second private key portion and the public key.

9. A system for asymmetrically transforming a message, comprising:

a first processor representing a user and configured to generate, based on a password of the user, a first portion of a private crypto-key, to transform a message with the first private key portion, and to destroy the generated private key portion after transforming the message and;

a second processor configured to further transform the transformed message by applying at least one of a second portion of the private crypto-key and a public crypto-key, both of which correspond to the first private key portion.

10. A system according to claim 9, further comprising:

a storage device configured to store the second private key portion and the public crypto-key in a persistent state;

wherein the applied at least one of a second portion of the private crypto-key and a public crypto-key is at least one of the stored second private key portion and the stored public crypto-key, and the second processor is further configured to retrieve the at least one of the stored second private key portion and the stored public crypto-key based on the user password;

wherein the first private key portion is never stored in a persistent state.

11. A system according to claim 9, wherein the user password has a bit length of between 56 and 72 bits and the generated first private key portion has a bit length of at least 257 bits.

12. A system according to claim 9, wherein the first private key portion is generated in accordance with a one way function.

13. A system according to claim 12, wherein:

the first processor and the second processor are further configured to selectively operate in a first mode and a second mode;

in the first mode the first processor and the second processor apply the one way function a first number of times to generate the first private key portion; and

in the second mode the first processor and the second processor apply the one way function a second number of times, different than the first number of times, to generate the first private key portion.

14. A system according to claim 31, wherein:

the first processor and the second processor are further configured to select one of the first and second mode for operation based on at least one of an identity of the user and a strength of the user password.

15. A system according to claim 12, wherein:

the first processor and the second processor are further configured to select the one way function from a group of one way functions.

16. A system according to claim 15, wherein:

the first processor and the second processor are further configured to select the one way function based upon at least one of an identity of the user and a strength of the user password

17. A system for communicating a transformed message, in which a user is associated with a private crypto-key and a corresponding public crypto-key, and the private crypto-key has a first private key portion and a second private key portion, comprising:

a first networked device, representing the user, configured to generate the first private key portion, to transform a first message with the generated first private key portion to form a second message, and to transmit the second message;

a second networked device configured to store the public crypto-key and the second private key portion, to receive the second message, and to further transform the second message with the second private portion to obtain the first message;

wherein the first private portion is (i) not stored at any networked device and (ii) not transmitted over the network.

18. A method for generating an asymmetric crypto-key usable to transform messages to both encrypt and decrypt the messages for a user, comprising:

generating, based upon a password of the user, a private crypto-key and a corresponding public crypto-key associated with the user;

dividing the private crypto-key into a first private key portion and a second private key portion;

destroying the private crypto-key and the first private key portion without distribution thereof and without storage thereof in a persistent state;

separately generating, responsive to receipt of, and based upon, the user password, only the first private key portion; and

destroying, without storing in a persistent state, the separately generated first private key portion.

19. The method according to claim 18, wherein the password has a bit length of 56 to 72 bits and the generated first private key portion has a bit length of at least 257 bits.

20. The method according to claim 18, wherein the first private key portion is generated in accordance with a one way function.

21. The method according to claim 18, further comprising:

selecting one of a first mode and a second mode in which to

generate the first private key portion in accordance with a one way function;

wherein the first mode the one way function is applied to the password a first number of times to generate the first private key portion; and

wherein the second mode the one way function is applied to the password a second number of times, different than the first number of times, to generate the first private key portion.

22. The method according to claim 21, wherein selection of the first and second mode is based on at least one of an identity of the user and a strength of the user password.

23. The method according to claim 18, further comprising:

selecting a one way function from a group of one way functions; and

generating the first private key portion in accordance with the selected one way function;

wherein selection of the one way function is based upon at least one of an identity of the user and a strength of the user password.

24. The method according to claim 18, further comprising:

transforming a message with the generated first private key portion prior to destruction thereof; and

further transforming the message by applying at least one of the second private key portion and the public crypto-key.

25. The method according to claim 24, further comprising:

storing the second private key portion and the public crypto-key in a persistent state; and

retrieving the at least one of the stored second private key portion and the stored public crypto-key;

wherein the applied at least one of the second private key portion and the public crypto-key is at least one of the retrieved at least one of the second private key portion and the public crypto-key; and

wherein the first private key portion is never stored in a persistent state.

26. A method for communicating a transformed message, in which a user is associated with a private crypto-key and a corresponding public crypto-key, and the private crypto-key has a first private key portion and a second private key portion, comprising:

generating the first private key portion and transforming a first message with the generated first private key portion;

further transforming the first message with the second private portion;

wherein the first private portion is (i) not stored at any networked device and (ii) not transmitted over a network.

27. The method according to claim 26, further comprising:

processing a password to generate the first private key portion;

wherein the password has a bit length of 56 to 72 bits and the generated first private key portion has a bit length of at least 257 bits.

28. The method according to claim 27, wherein the first private key portion is generated in accordance with a one way function.

29. The method according to claim 27, further comprising:

selecting one of a first mode and a second mode in which to generate the first private key portion in accordance with a one way function;

wherein the first mode the one way function is applied to the password a first number of times to generate the first private key portion; and

wherein the second mode the one way function is applied to the password a second number of times, different than the first number of times, to generate the first private key portion.

30. The method according to claim 29, wherein selection of the first and second mode is based on at least one of an identity of the user and a strength of the user password.

31. The method according to claim 27, further comprising:

selecting a one way function from a group of one way functions; and

generating the first private key portion in accordance with the selected one way function;

wherein selection of the one way function is based upon at least one of an identity of the user and a strength of the user password.